

PATENT ABSTRACTS OF JAPAN

(11)Publication number : 2000-215165

(43)Date of publication of application : 04.08.2000

(51)Int.Cl.

G06F 15/00
G06F 12/14
G06F 17/60
G09C 1/00
H04L 9/32

(21)Application number : 11-017401

(71)Applicant : NIPPON TELEGR & TELEPH
CORP <NTT>

(22)Date of filing : 26.01.1999

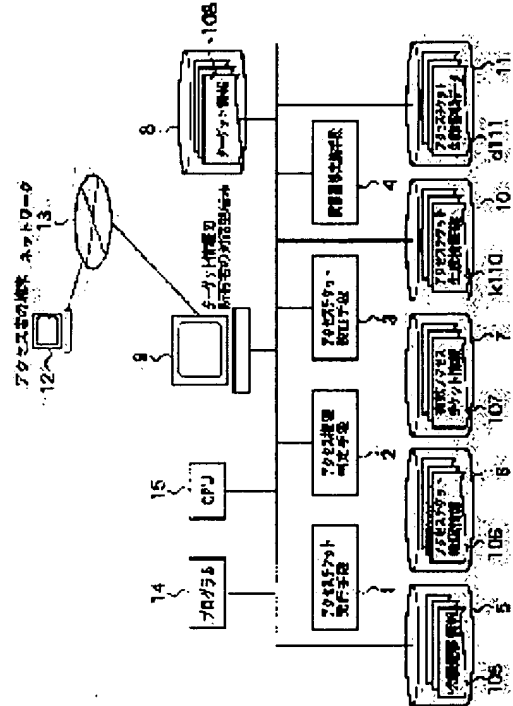
(72)Inventor : OSHIMA YOSHITO
OHARA YASUHIRO

(54) METHOD AND DEVICE FOR INFORMATION ACCESS CONTROL AND RECORD MEDIUM RECORDING INFORMATION ACCESS CONTROL PROGRAM

(57)Abstract:

PROBLEM TO BE SOLVED: To provide the method and device for information access control which can easily change the access authority to be allowed to an accessing person in response to the change of situation of a transaction and also to provide a recording medium which records an information access control program.

SOLUTION: An access ticket issuing means 1 issues the access tickets to every accessing person and these tickets prescribe the access authority to the target information for each of plural types and states. Receiving an access request from an accessing person, the means 1 reads the request and the access authority corresponding to the type and state of an inputted access ticket out of an access ticket authority information storing means 6 and decides to permit or not permit the access request based on the access authority. When a state transition request is received from the accessing person, the transition destination state is read out of a state transition information storing means 5 based on the type and state of the access ticket that is inputted together with the state transition request. Based on the transition destination state, the change of the access ticket is updated.



(11)特許出願公開番号

(P2000-215165A)

(43)公開日 平成12年8月4日(2000.8.4)

(51)Int.Cl. ⁷	識別記号	F I	テロトド(参考)
G 0 6 F 15/00	3 3 0	G 0 6 F 15/00	3 3 0 A 5 B 0 1 7
12/14	3 1 0	12/14	3 1 0 K 5 B 0 4 9
17/60		G 0 9 C 1/00	6 6 0 E 5 B 0 8 5
G 0 9 C 1/00	6 6 0	G 0 6 F 15/21	Z 5 J 1 0 4
H 0 4 L 9/32		H 0 4 L 9/00	6 7 1 9 A 0 0 1

審査請求 未請求 請求項の数24 O L (全 23 頁)

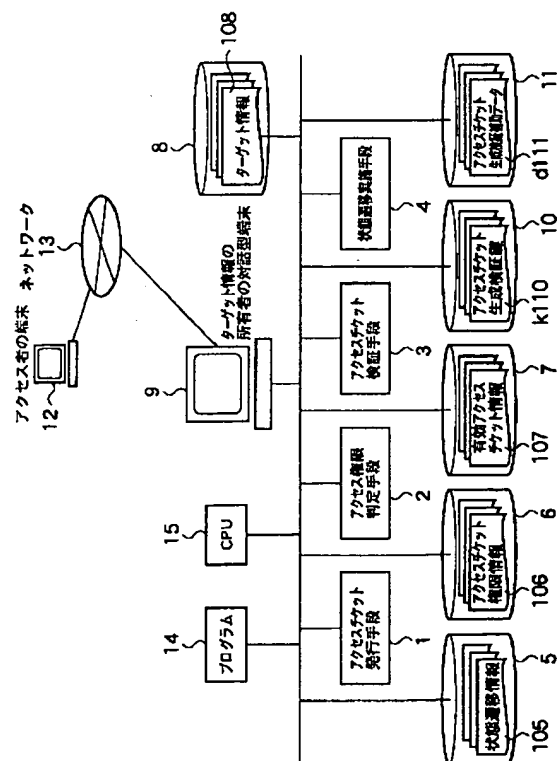
最終頁に続く

(54) 【発明の名称】 情報アクセス制御方法および装置と情報アクセス制御プログラムを記録した記録媒体

(57) 【要約】

【課題】 アクセス者に対して許容するアクセス権限を取引の局面で変化に応じて容易に変更することができる情報アクセス制御方法および装置と情報アクセス制御プログラムを記録した記録媒体を提供する。

【解決手段】 アクセスチケット発行手段1で複数の種類の複数の状態の各々毎にターゲット情報へのアクセス権限を規定しているアクセスチケットを各アクセス者に発行し、アクセス者からのアクセス要求を受け付けると、この要求とともに入力されたアクセスチケットの種類および状態に対応するアクセス権限をアクセスチケット権限情報格納手段6から読み出し、このアクセス権限に基づいてアクセス要求を許可するか否かを判定し、アクセス者からの状態遷移要求を受け付けると、この要求とともに入力されたアクセスチケットの種類および状態に基づいて遷移先状態を状態遷移情報格納手段5から読み出し、この遷移先状態でアクセスチケットの状態を更新する。



【特許請求の範囲】

【請求項1】 保護対象資源であるターゲット情報にアクセスするアクセス者のアクセスを制御する情報アクセス制御方法であって、

複数の状態を取ることができ、この複数の状態の各々毎にターゲット情報へのアクセス権限を規定しているアクセスチケットを各アクセス者に発行し、

アクセス者からのアクセス要求を受け付け、この要求とともに入力されたアクセスチケットの状態に対応して規定されているアクセス権限に基づいて前記アクセス要求を許可するか否かを判定し、

アクセス者からの状態遷移要求を受け付け、この要求とともに入力されたアクセスチケットの状態に基づいて遷移先状態を決定し、この決定した遷移先状態でアクセスチケットの状態を更新することを特徴とする情報アクセス制御方法。

【請求項2】 保護対象資源であるターゲット情報にアクセスするアクセス者のアクセスを制御する情報アクセス制御方法であって、

アクセスの内容に応じた複数の種類が設けられるとともに、各種類において複数の状態を取ることができ、各種類における複数の状態の各々毎にターゲット情報へのアクセス権限を規定しているアクセスチケットを各アクセス者に発行し、

アクセス者からのアクセス要求を受け付け、この要求とともに入力されたアクセスチケットの種類および状態に対応して規定されているアクセス権限に基づいて前記アクセス要求を許可するか否かを判定し、

アクセス者からの状態遷移要求を受け付け、この要求とともに入力されたアクセスチケットの種類および状態に基づいて遷移先状態を決定し、この決定した遷移先状態でアクセスチケットの状態を更新することを特徴とする情報アクセス制御方法。

【請求項3】 前記アクセスチケットの状態を更新する処理は、アクセスチケットの各状態が遷移する遷移先状態を各状態に対応して状態遷移情報格納テーブルに格納しておき、アクセス者からの前記状態遷移要求とともに入力されたアクセスチケットの状態に対応する遷移先状態を前記状態遷移情報格納テーブルから読み出し、この読み出した遷移先状態でアクセスチケットの状態を更新することを特徴とする請求項1記載の情報アクセス制御方法。

【請求項4】 前記アクセスチケットの状態を更新する処理は、各種類のアクセスチケットの各状態が遷移する遷移先状態をアクセスチケットの複数の種類の複数の状態の各々に対応して状態遷移情報格納テーブルに格納しておき、アクセス者から前記状態遷移要求とともに入力されたアクセスチケットの種類および状態に対応する遷移先状態を前記状態遷移情報格納テーブルから読み出し、この読み出した遷移先状態でアクセスチケットの状

態を更新することを特徴とする請求項2記載の情報アクセス制御方法。

【請求項5】 前記アクセスチケットの状態を更新する処理は、アクセス者からの前記状態遷移要求に状態遷移イベントが含まれており、この状態遷移イベントも考慮して前記遷移先状態を決定していることを特徴とする請求項1乃至4のいずれかに記載の情報アクセス制御方法。

【請求項6】 前記要求とともに入力されるアクセスチケットが有効か否かを検証することを特徴とする請求項1または2記載の情報アクセス制御方法。

【請求項7】 前記アクセス要求を許可するか否かを判定する処理は、アクセスチケットの各状態に対応して規定されるアクセス権限をアクセスチケット権限情報格納テーブルに格納しておき、前記アクセス要求とともに入力されるアクセスチケットの状態に対応して規定されているアクセス権限を前記アクセスチケット権限情報格納テーブルから読み出し、この読み出したアクセス権限に基づいて前記アクセス要求を許可するか否かを判定することを特徴とする請求項1記載の情報アクセス制御方法。

【請求項8】 前記アクセス要求を許可するか否かを判定する処理は、アクセスチケットの複数の種類の複数の状態の各々に対応して規定されるアクセス権限をアクセスチケット権限情報格納テーブルに格納しておき、前記アクセス要求とともに入力されるアクセスチケットの種類および状態に対応して規定されているアクセス権限を前記アクセスチケット権限情報格納テーブルから読み出し、この読み出したアクセス権限に基づいて前記アクセス要求を許可するか否かを判定することを特徴とする請求項2記載の情報アクセス制御方法。

【請求項9】 保護対象資源であるターゲット情報にアクセスするアクセス者のアクセスを制御する情報アクセス制御装置であって、

複数の状態を取ることができ、この複数の状態の各々毎にターゲット情報へのアクセス権限を規定しているアクセスチケットを各アクセス者に発行するアクセスチケット発行手段と、

アクセス者からのアクセス要求を受け付け、この要求とともに入力されたアクセスチケットの状態に対応して規定されているアクセス権限に基づいて前記アクセス要求を許可するか否かを判定するアクセス権限判定手段と、アクセス者からの状態遷移要求を受け付け、この要求とともに入力されたアクセスチケットの状態に基づいて遷移先状態を決定し、この決定した遷移先状態でアクセスチケットの状態を更新する状態更新手段とを有することを特徴とする情報アクセス制御装置。

【請求項10】 保護対象資源であるターゲット情報にアクセスするアクセス者のアクセスを制御する情報アクセス制御装置であって、

10

20

30

40

50

アクセスの内容に応じた複数の種類が設けられるとともに、各種類において複数の状態を取ることができ、各種類における複数の状態の各々毎にターゲット情報へのアクセス権限を規定しているアクセスチケットを各アクセス者に発行するアクセスチケット発行手段と、

アクセス者からのアクセス要求を受け付け、この要求とともに入力されたアクセスチケットの種類および状態に対応して規定されているアクセス権限に基づいて前記アクセス要求を許可するか否かを判定するアクセス権限判定手段と、

アクセス者からの状態遷移要求を受け付け、この要求とともに入力されたアクセスチケットの種類および状態に基づいて遷移先状態を決定し、この決定した遷移先状態でアクセスチケットの状態を更新する状態更新手段とを有することを特徴とする情報アクセス制御装置。

【請求項11】 前記状態更新手段は、アクセスチケットの各状態が遷移する遷移先状態を各状態に対応して格納している状態遷移情報格納手段と、アクセス者からの前記状態遷移要求とともに入力されたアクセスチケットの状態に対応する遷移先状態を前記状態遷移情報格納手段から読み出し、この読み出した遷移先状態でアクセスチケットの状態を更新する手段とを有することを特徴とする請求項9記載の情報アクセス制御装置。

【請求項12】 前記状態更新手段は、各種類のアクセスチケットの各状態が遷移する遷移先状態をアクセスチケットの複数の種類の複数の状態の各々に対応して格納している状態遷移情報格納手段と、アクセス者から前記状態遷移要求とともに入力されたアクセスチケットの種類および状態に対応する遷移先状態を前記状態遷移情報格納手段から読み出し、この読み出した遷移先状態でアクセスチケットの状態を更新する手段とを有することを特徴とする請求項10記載の情報アクセス制御装置。

【請求項13】 前記状態更新手段は、アクセス者からの前記状態遷移要求に含まれている状態遷移イベントも考慮して前記遷移先状態を決定する手段を有することを特徴とする請求項9乃至12のいずれかに記載の情報アクセス制御装置。

【請求項14】 前記要求とともに入力されるアクセスチケットが有効か否かを検証するアクセスチケット検証手段を有することを特徴とする請求項9または10記載の情報アクセス制御装置。

【請求項15】 前記アクセス権限判定手段は、アクセスチケットの各状態に対応して規定されるアクセス権限を格納しているアクセスチケット権限情報格納手段と、前記アクセス要求とともに入力されるアクセスチケットの状態に対応して規定されているアクセス権限を前記アクセスチケット権限情報格納手段から読み出し、この読み出したアクセス権限に基づいて前記アクセス要求を許可するか否かを判定する手段とを有することを特徴とする請求項9記載の情報アクセス制御装置。

【請求項16】 前記アクセス権限判定手段は、アクセスチケットの複数の種類の複数の状態の各々に対応して規定されるアクセス権限を格納しているアクセスチケット権限情報格納手段と、前記アクセス要求とともに入力されるアクセスチケットの種類および状態に対応して規定されているアクセス権限を前記アクセスチケット権限情報格納手段から読み出し、この読み出したアクセス権限に基づいて前記アクセス要求を許可するか否かを判定する手段とを有することを特徴とする請求項10記載の情報アクセス制御装置。

【請求項17】 保護対象資源であるターゲット情報にアクセスするアクセス者のアクセスを制御する情報アクセス制御プログラムを記録した記録媒体であって、複数の状態を取ることができ、この複数の状態の各々毎にターゲット情報へのアクセス権限を規定しているアクセスチケットを各アクセス者に発行し、

アクセス者からのアクセス要求を受け付け、この要求とともに入力されたアクセスチケットの状態に対応して規定されているアクセス権限に基づいて前記アクセス要求を許可するか否かを判定し、

アクセス者からの状態遷移要求を受け付け、この要求とともに入力されたアクセスチケットの状態に基づいて遷移先状態を決定し、この決定した遷移先状態でアクセスチケットの状態を更新することを特徴とする情報アクセス制御プログラムを記録した記録媒体。

【請求項18】 保護対象資源であるターゲット情報にアクセスするアクセス者のアクセスを制御する情報アクセス制御プログラムを記録した記録媒体であって、アクセスの内容に応じた複数の種類が設けられるとともに、各種類において複数の状態を取ることができ、各種類における複数の状態の各々毎にターゲット情報へのアクセス権限を規定しているアクセスチケットを各アクセス者に発行し、

アクセス者からのアクセス要求を受け付け、この要求とともに入力されたアクセスチケットの種類および状態に対応して規定されているアクセス権限に基づいて前記アクセス要求を許可するか否かを判定し、

アクセス者からの状態遷移要求を受け付け、この要求とともに入力されたアクセスチケットの種類および状態に基づいて遷移先状態を決定し、この決定した遷移先状態でアクセスチケットの状態を更新することを特徴とする情報アクセス制御プログラムを記録した記録媒体。

【請求項19】 前記アクセスチケットの状態を更新する処理は、アクセスチケットの各状態が遷移する遷移先状態を各状態に対応して状態遷移情報格納テーブルに格納しておき、アクセス者からの前記状態遷移要求とともに入力されたアクセスチケットの状態に対応する遷移先状態を前記状態遷移情報格納テーブルから読み出し、この読み出した遷移先状態でアクセスチケットの状態を更新することを特徴とする請求項17記載の情報アクセス

制御プログラムを記録した記録媒体。

【請求項20】 前記アクセスチケットの状態を更新する処理は、各種類のアクセスチケットの各状態が遷移する遷移先状態をアクセスチケットの複数の種類の複数の状態の各々に対応して状態遷移情報格納テーブルに格納しておき、アクセス者から前記状態遷移要求とともに入力されたアクセスチケットの種類および状態に対応する遷移先状態を前記状態遷移情報格納テーブルから読み出し、この読み出した遷移先状態でアクセスチケットの状態を更新することを特徴とする請求項18記載の情報アクセス制御プログラムを記録した記録媒体。

【請求項21】 前記アクセスチケットの状態を更新する処理は、アクセス者からの前記状態遷移要求に状態遷移イベントが含まれており、この状態遷移イベントも考慮して前記遷移先状態を決定していることを特徴とする請求項17乃至20のいずれかに記載の情報アクセス制御プログラムを記録した記録媒体。

【請求項22】 前記要求とともに入力されるアクセスチケットが有効か否かを検証することを特徴とする請求項17または18記載の情報アクセス制御プログラムを記録した記録媒体。

【請求項23】 前記アクセス要求を許可するか否かを判定する処理は、アクセスチケットの各状態に対応して規定されるアクセス権限をアクセスチケット権限情報格納テーブルに格納しておき、前記アクセス要求とともに入力されるアクセスチケットの状態に対応して規定されているアクセス権限を前記アクセスチケット権限情報格納テーブルから読み出し、この読み出したアクセス権限に基づいて前記アクセス要求を許可するか否かを判定することを特徴とする請求項17記載の情報アクセス制御プログラムを記録した記録媒体。

【請求項24】 前記アクセス要求を許可するか否かを判定する処理は、アクセスチケットの複数の種類の複数の状態の各々に対応して規定されるアクセス権限をアクセスチケット権限情報格納テーブルに格納しておき、前記アクセス要求とともに入力されるアクセスチケットの種類および状態に対応して規定されているアクセス権限を前記アクセスチケット権限情報格納テーブルから読み出し、この読み出したアクセス権限に基づいて前記アクセス要求を許可するか否かを判定することを特徴とする請求項18記載の情報アクセス制御プログラムを記録した記録媒体。

【発明の詳細な説明】

【0001】

【発明の属する技術分野】本発明は、保護対象資源であるターゲット情報にアクセスするアクセス者のアクセスを制御する情報アクセス制御方法および装置に関し、更に詳しくは、インターネットのような不特定多数のユーザが参加する開放型分散システムにおいてあるユーザが自身の管理する保護対象資源であるターゲット情報に

する他のユーザであるアクセス者によるアクセスを制御すべく制御する情報アクセス制御方法および装置と情報アクセス制御プログラムを記録した記録媒体に関する。特に、本発明は、インターネット上での商取引のようにアクセス者それぞれの目的や役割が取引の局面に応じて変化するために同一のアクセス者に対しても取引の局面の変化に応じて許容するアクセス権限を違える必要があるといった特徴を持つシステムにおける保護対象資源へのアクセスを制御する情報アクセス制御方法および装置と情報アクセス制御プログラムを記録した記録媒体に関する。

【0002】

【従来の技術】一般に、保護対象資源（ターゲット情報）に対するアクセス制御は、アクセスを試みる主体（アクセス者）と、アクセスされる保護対象資源、ターゲット情報に対するアクセスの種別のセットで記述されたアクセス権限情報に基づいて実施される。アクセス権限情報に基づくアクセス制御の方法として、アクセス制御リスト（ACL）に基づくアクセス制御の方法と、アクセス資格（ケイパビリティ）に基づく方法とがある。

【0003】前者は、個々のターゲット情報毎に、そのターゲット情報に対するアクセスが許容されるアクセス者およびそのアクセスの種別を対にして並べた一覧（ACL）に基づいて制御する方法であり、アクセス要求が発生する毎にACLを探索し、そのアクセス要求を許可するか否かを決定する。これを拡張した方法として、ロールに基づくアクセス制御の方法がある。この方法では、複数のアクセス者に同一のアクセス権限が許容する場合に、それらアクセス者をロールと呼ばれる単位にまとめ、各ロールに対するアクセス権限を記述・管理する。

【0004】一方、後者は、あるターゲット情報に対するある種別のアクセスを行うアクセス権限を表すデータ（ケイパビリティ）を用いて制御する方法であり、アクセス要求の内容を含むアクセス権限を表すケイパビリティがアクセス者から提示された場合に、そのアクセス要求を許可する。ケイパビリティの無効リストなどを用いて、発行済みケイパビリティの無効／有効を制御することも可能である。このケイパビリティに基づく方法では、アクセス要求が発生する毎に、ACLを探索する必要はない。

【0005】

【発明が解決しようとする課題】誰でもが自由に参加できるインターネット上での商取引のように、不特定多数のアクセス者が想定され、またアクセス者それぞれの目的や役割が取引の局面に応じて変化するために、同一のアクセス者に対しても、取引の局面の変化に応じて、許容するアクセス権限を違える必要があるといった特徴を持つ環境においては、上述した従来のアクセス制御の方法では、以下のような問題が生ずる。

【0006】まず、ACLあるいはロールに基づくアクセス制御の方法では、アクセス者へのアクセス権限の割り当て、あるいは、アクセス者へのロールの割り当ておよびロールへのアクセス権限の割り当ては固定的なものであり、同一のアクセス者に許容するアクセス権限を取引の局面の変化に応じて変更することはできない。

【0007】また、ケイパビリティに基づくアクセス制御の方法では、同じアクセス者に対しても、取引の局面が変化する度に、新しい局面に応じたケイパビリティを発行・付与したり、また発行・付与済みのケイパビリティを無効化したりする必要がある。

【0008】このため、アクセス制御側でのケイパビリティ発行数の増加による発行・付与処理コストの増加、および発行済みケイパビリティの制御・管理の煩雑化、およびアクセス者側での、保有しなければならないケイパビリティ数の増加によるケイパビリティの管理コストおよび適切なケイパビリティを使い分けるための処理コストの増加といった問題が生じる。

【0009】本発明は、上記に鑑みてなされたもので、その目的とするところは、アクセス者に対して許容するアクセス権限を取引の局面の変化に応じて容易に変更することができる情報アクセス制御方法および装置と情報アクセス制御プログラムを記録した記録媒体を提供することにある。

【0010】

【課題を解決するための手段】上記目的を達成するため、請求項1記載の本発明は、保護対象資源であるターゲット情報にアクセスするアクセス者のアクセスを制御する情報アクセス制御方法であって、複数の状態を取ることができ、この複数の状態の各々毎にターゲット情報へのアクセス権限を規定しているアクセスチケットを各アクセス者に発行し、アクセス者からのアクセス要求を受け付け、この要求とともに入力されたアクセスチケットの状態に対応して規定されているアクセス権限に基づいて前記アクセス要求を許可するか否かを判定し、アクセス者からの状態遷移要求を受け付け、この要求とともに入力されたアクセスチケットの状態に基づいて遷移先状態を決定し、この決定した遷移先状態でアクセスチケットの状態を更新することを要旨とする。

【0011】請求項1記載の本発明にあつては、各状態毎にターゲット情報へのアクセス権限を規定しているアクセスチケットを各アクセス者に発行し、アクセス要求を受け付けた場合、該要求とともに入力されたアクセスチケットの状態に対して規定されているアクセス権限に基づいてアクセス要求を許可するか否かを判定し、アクセス者からの状態遷移要求を受け付けた場合、該要求とともに入力されたアクセスチケットの状態に基づいて遷移先状態を決定し、この遷移先状態でアクセスチケットの状態を更新するため、アクセス者に対して許容するアクセス権限を取引の局面の変化に応じて容易に変更で

き、柔軟なアクセス制御を実現することができる。

【0012】また、請求項2記載の本発明は、保護対象資源であるターゲット情報にアクセスするアクセス者のアクセスを制御する情報アクセス制御方法であつて、アクセスの内容に応じた複数の種類が設けられるとともに、各種類において複数の状態を取ることができ、各種類における複数の状態の各々毎にターゲット情報へのアクセス権限を規定しているアクセスチケットを各アクセス者に発行し、アクセス者からのアクセス要求を受け付け、この要求とともに入力されたアクセスチケットの種類および状態に対応して規定されているアクセス権限に基づいて前記アクセス要求を許可するか否かを判定し、アクセス者からの状態遷移要求を受け付け、この要求とともに入力されたアクセスチケットの種類および状態に基づいて遷移先状態を決定し、この決定した遷移先状態でアクセスチケットの状態を更新することを要旨とする。

【0013】請求項2記載の本発明にあつては、複数の種類の複数の状態の各々毎にターゲット情報へのアクセス権限を規定しているアクセスチケットを各アクセス者に発行し、アクセス要求を受け付けた場合、アクセスチケットの種類および状態に対して規定されているアクセス権限に基づいてアクセス要求を許可するか否かを判定し、また状態遷移要求を受け付けた場合、アクセスチケットの種類および状態に基づいて遷移先状態を決定し、この決定した遷移先状態でアクセスチケットの状態を更新するため、アクセス者に対して許容するアクセス権限を取引の局面の変化に応じて容易に変更でき、柔軟なアクセス制御を実現することができる。

【0014】更に、請求項3記載の本発明は、請求項1記載の発明において、前記アクセスチケットの状態を更新する処理が、アクセスチケットの各状態が遷移する遷移先状態を各状態に対応して状態遷移情報格納テーブルに格納しておき、アクセス者からの前記状態遷移要求とともに入力されたアクセスチケットの状態に対応する遷移先状態を前記状態遷移情報格納テーブルから読み出し、この読み出した遷移先状態でアクセスチケットの状態を更新することを要旨とする。

【0015】請求項3記載の本発明にあつては、アクセスチケットの各状態の遷移先状態を状態遷移情報格納テーブルに格納しておき、アクセス者からの状態遷移要求の入力時、状態遷移情報格納テーブルからアクセスチケットの状態に対応する遷移先状態を読み出し、この遷移先状態でアクセスチケットの状態を更新する。

【0016】請求項4記載の本発明は、請求項2記載の発明において、前記アクセスチケットの状態を更新する処理が、各種類のアクセスチケットの各状態が遷移する遷移先状態をアクセスチケットの複数の種類の複数の状態の各々に対応して状態遷移情報格納テーブルに格納しておき、アクセス者から前記状態遷移要求とともに入力

されたアクセスチケットの種類および状態に対応する遷移先状態を前記状態遷移情報格納テーブルから読み出し、この読み出した遷移先状態でアクセスチケットの状態を更新することを要旨とする。

【0017】請求項4記載の本発明にあつては、各種類のアクセスチケットの各状態の遷移先状態を状態遷移情報格納テーブルに格納しておき、アクセス者から状態遷移要求の入力時、アクセスチケットの種類および状態に対応する遷移先状態を状態遷移情報格納テーブルから読み出し、この遷移先状態でアクセスチケットの状態を更新する。

【0018】また、請求項5記載の本発明は、請求項1乃至4のいずれかに記載の発明において、前記アクセスチケットの状態を更新する処理が、アクセス者からの前記状態遷移要求に状態遷移イベントが含まれており、この状態遷移イベントも考慮して前記遷移先状態を決定していることを要旨とする。

【0019】請求項5記載の本発明にあつては、アクセス者からの状態遷移要求に状態遷移イベントが含まれており、この状態遷移イベントも考慮して遷移先状態を決定している。

【0020】更に、請求項6記載の本発明は、請求項1または2記載の発明において、前記要求とともに入力されるアクセスチケットが有効か否かを検証することを要旨とする。

【0021】請求項6記載の本発明にあつては、状態遷移要求やアクセス要求等の要求とともに入力されるアクセスチケットが有効か否かを検証している。

【0022】請求項7記載の本発明は、請求項1記載の発明において、前記アクセス要求を許可するか否かを判定する処理が、アクセスチケットの各状態に対応して規定されるアクセス権限をアクセスチケット権限情報格納テーブルに格納しておき、前記アクセス要求とともに入力されるアクセスチケットの状態に対応して規定されているアクセス権限を前記アクセスチケット権限情報格納テーブルから読み出し、この読み出したアクセス権限に基づいて前記アクセス要求を許可するか否かを判定することを要旨とする。

【0023】請求項7記載の本発明にあつては、アクセスチケットの各状態に対応するアクセス権限をアクセスチケット権限情報格納テーブルに格納しておき、アクセス要求時、アクセスチケットの状態に対応するアクセス権限をアクセスチケット権限情報格納テーブルから読み出し、このアクセス権限に基づいてアクセス要求を許可するか否かを判定している。

【0024】また、請求項8記載の本発明は、請求項2または4記載の発明において、前記アクセス要求を許可するか否かを判定する処理が、アクセスチケットの複数の種類の複数の状態の各々に対応して規定されるアクセス権限をアクセスチケット権限情報格納テーブルに格納

しておき、前記アクセス要求とともに入力されるアクセスチケットの種類および状態に対応して規定されているアクセス権限を前記アクセスチケット権限情報格納テーブルから読み出し、この読み出したアクセス権限に基づいて前記アクセス要求を許可するか否かを判定することを要旨とする。

【0025】請求項8記載の本発明にあつては、アクセスチケットの複数の種類の複数の状態の各々に対応するアクセス権限をアクセスチケット権限情報格納テーブルに格納しておき、アクセス要求時、アクセスチケットの種類および状態に対応するアクセス権限をアクセスチケット権限情報格納テーブルから読み出し、このアクセス権限に基づいてアクセス要求を許可するか否かを判定している。

【0026】更に、請求項9記載の本発明は、保護対象資源であるターゲット情報にアクセスするアクセス者のアクセスを制御する情報アクセス制御装置であつて、複数の状態を取ることができ、この複数の状態の各々毎にターゲット情報へのアクセス権限を規定しているアクセスチケットを各アクセス者に発行するアクセスチケット発行手段と、アクセス者からのアクセス要求を受け付け、この要求とともに入力されたアクセスチケットの状態に対応して規定されているアクセス権限に基づいて前記アクセス要求を許可するか否かを判定するアクセス権限判定手段と、アクセス者からの状態遷移要求を受け付け、この要求とともに入力されたアクセスチケットの状態に基づいて遷移先状態を決定し、この決定した遷移先状態でアクセスチケットの状態を更新する状態更新手段とを有することを要旨とする。

【0027】請求項9記載の本発明にあつては、各状態毎にターゲット情報へのアクセス権限を規定しているアクセスチケットを各アクセス者に発行し、アクセス要求を受け付けた場合、該要求とともに入力されたアクセスチケットの状態に対して規定されているアクセス権限に基づいてアクセス要求を許可するか否かを判定し、アクセス者からの状態遷移要求を受け付けた場合、該要求とともに入力されたアクセスチケットの状態に基づいて遷移先状態を決定し、この遷移先状態でアクセスチケットの状態を更新するため、アクセス者に対して許容するアクセス権限を取引の局面の変化に応じて容易に変更でき、柔軟なアクセス制御を実現することができる。

【0028】請求項10記載の本発明は、保護対象資源であるターゲット情報にアクセスするアクセス者のアクセスを制御する情報アクセス制御装置であつて、アクセスの内部に応じた複数の種類が設けられるとともに、各種類において複数の状態を取ることができ、各種類における複数の状態の各々毎にターゲット情報へのアクセス権限を規定しているアクセスチケットを各アクセス者に発行するアクセスチケット発行手段と、アクセス者からのアクセス要求を受け付け、この要求とともに入力され

たアクセスチケットの種類および状態に対応して規定されているアクセス権限に基づいて前記アクセス要求を許可するか否かを判定するアクセス権限判定手段と、アクセス者からの状態遷移要求を受け付け、この要求とともに入力されたアクセスチケットの種類および状態に基づいて遷移先状態を決定し、この決定した遷移先状態でアクセスチケットの状態を更新する状態更新手段とを有することを要旨とする。

【0029】請求項10記載の本発明にあつては、複数の種類の複数の状態の各々毎にターゲット情報へのアクセス権限を規定しているアクセスチケットを各アクセス者に発行し、アクセス要求を受け付けた場合、アクセスチケットの種類および状態に対して規定されているアクセス権限に基づいてアクセス要求を許可するか否かを判定し、また状態遷移要求を受け付けた場合、アクセスチケットの種類および状態に基づいて遷移先状態を決定し、この決定した遷移先状態でアクセスチケットの状態を更新するため、アクセス者に対して許容するアクセス権限を取引の局面の変化に応じて容易に変更でき、柔軟なアクセス制御を実現することができる。

【0030】また、請求項11記載の本発明は、請求項9記載の発明において、前記状態更新手段が、アクセスチケットの各状態が遷移する遷移先状態を各状態に対応して格納している状態遷移情報格納手段と、アクセス者からの前記状態遷移要求とともに入力されたアクセスチケットの状態に対応する遷移先状態を前記状態遷移情報格納手段から読み出し、この読み出した遷移先状態でアクセスチケットの状態を更新する手段とを有することを要旨とする。

【0031】請求項11記載の本発明にあつては、アクセスチケットの各状態の遷移先状態を状態遷移情報格納手段に格納しておき、アクセス者からの状態遷移要求の入力時、状態遷移情報格納手段からアクセスチケットの状態に対応する遷移先状態を読み出し、この遷移先状態でアクセスチケットの状態を更新する。

【0032】更に、請求項12記載の本発明は、請求項10記載の発明において、前記状態更新手段が、各種類のアクセスチケットの各状態が遷移する遷移先状態をアクセスチケットの複数の種類の複数の状態の各々に対応して格納している状態遷移情報格納手段と、アクセス者から前記状態遷移要求とともに入力されたアクセスチケットの種類および状態に対応する遷移先状態を前記状態遷移情報格納手段から読み出し、この読み出した遷移先状態でアクセスチケットの状態を更新する手段とを有することを要旨とする。

【0033】請求項12記載の本発明にあつては、各種類のアクセスチケットの各状態の遷移先状態を状態遷移情報格納手段に格納しておき、アクセス者から状態遷移要求の入力時、アクセスチケットの種類および状態に対応する遷移先状態を状態遷移情報格納手段から読み出

し、この遷移先状態でアクセスチケットの状態を更新する。

【0034】請求項13記載の本発明は、請求項9乃至12のいずれかに記載の発明において、前記状態更新手段が、アクセス者からの前記状態遷移要求に含まれている状態遷移イベントも考慮して前記遷移先状態を決定する手段を有することを要旨とする。

【0035】請求項13記載の本発明にあつては、アクセス者からの状態遷移要求に状態遷移イベントが含まれており、この状態遷移イベントも考慮して遷移先状態を決定している。

【0036】また、請求項14記載の本発明は、請求項9または10記載の発明において、前記要求とともに入力されるアクセスチケットが有効か否かを検証するアクセスチケット検証手段を有することを要旨とする。

【0037】請求項14記載の本発明にあつては、状態遷移要求やアクセス要求等の要求とともに入力されるアクセスチケットが有効か否かを検証している。

【0038】更に、請求項15記載の本発明は、請求項9記載の発明において、前記アクセス権限判定手段が、アクセスチケットの各状態に対応して規定されるアクセス権限を格納しているアクセスチケット権限情報格納手段と、前記アクセス要求とともに入力されるアクセスチケットの状態に対応して規定されているアクセス権限を前記アクセスチケット権限情報格納手段から読み出し、この読み出したアクセス権限に基づいて前記アクセス要求を許可するか否かを判定する手段とを有することを要旨とする。

【0039】請求項15記載の本発明にあつては、アクセスチケットの各状態に対応するアクセス権限をアクセスチケット権限情報格納手段に格納しておき、アクセス要求時、アクセスチケットの状態に対応するアクセス権限をアクセスチケット権限情報格納手段から読み出し、このアクセス権限に基づいてアクセス要求を許可するか否かを判定している。

【0040】請求項16記載の本発明は、請求項10記載の発明において、前記アクセス権限判定手段が、アクセスチケットの複数の種類の複数の状態の各々に対応して規定されるアクセス権限を格納しているアクセスチケット権限情報格納手段と、前記アクセス要求とともに入力されるアクセスチケットの種類および状態に対応して規定されているアクセス権限を前記アクセスチケット権限情報格納手段から読み出し、この読み出したアクセス権限に基づいて前記アクセス要求を許可するか否かを判定する手段とを有することを要旨とする。

【0041】請求項16記載の本発明にあつては、アクセスチケットの複数の種類の複数の状態の各々に対応するアクセス権限をアクセスチケット権限情報格納手段に格納しておき、アクセス要求時、アクセスチケットの種類および状態に対応するアクセス権限をアクセスチケッ

ト権限情報格納手段から読み出し、このアクセス権限に基づいてアクセス要求を許可するか否かを判定している。

【0042】また、請求項17記載の本発明は、保護対象資源であるターゲット情報にアクセスするアクセス者のアクセスを制御する情報アクセス制御プログラムを記録した記録媒体であって、複数の状態を取ることができ、この複数の状態の各々毎にターゲット情報へのアクセス権限を規定しているアクセスチケットを各アクセス者に発行し、アクセス者からのアクセス要求を受け付け、この要求とともに入力されたアクセスチケットの状態に対応して規定されているアクセス権限に基づいて前記アクセス要求を許可するか否かを判定し、アクセス者からの状態遷移要求を受け付け、この要求とともに入力されたアクセスチケットの状態に基づいて遷移先状態を決定し、この決定した遷移先状態でアクセスチケットの状態を更新する情報アクセス制御プログラムを記録媒体に記録することを要旨とする。

【0043】請求項17記載の本発明にあっては、各状態毎にターゲット情報へのアクセス権限を規定しているアクセスチケットを各アクセス者に発行し、アクセス要求を受け付けた場合、該要求とともに入力されたアクセスチケットの状態に対して規定されているアクセス権限に基づいてアクセス要求を許可するか否かを判定し、アクセス者からの状態遷移要求を受け付けた場合、該要求とともに入力されたアクセスチケットの状態に基づいて遷移先状態を決定し、この遷移先状態でアクセスチケットの状態を更新する情報アクセス制御プログラムを記録媒体に記録しているため、該記録媒体を用いて、その流通性を高めることができる。

【0044】更に、請求項18記載の本発明は、保護対象資源であるターゲット情報にアクセスするアクセス者のアクセスを制御する情報アクセス制御プログラムを記録した記録媒体であって、アクセスの内容に応じた複数の種類が設けられるとともに、各種類において複数の状態を取ることができ、各種類における複数の状態の各々毎にターゲット情報へのアクセス権限を規定しているアクセスチケットを各アクセス者に発行し、アクセス者からのアクセス要求を受け付け、この要求とともに入力されたアクセスチケットの種類および状態に対応して規定されているアクセス権限に基づいて前記アクセス要求を許可するか否かを判定し、アクセス者からの状態遷移要求を受け付け、この要求とともに入力されたアクセスチケットの種類および状態に基づいて遷移先状態を決定し、この決定した遷移先状態でアクセスチケットの状態を更新する情報アクセス制御プログラムを記録媒体に記録することを要旨とする。

【0045】請求項18記載の本発明にあっては、複数の種類の複数の状態の各々毎にターゲット情報へのアクセス権限を規定しているアクセスチケットを各アクセス

者に発行し、アクセス要求を受け付けた場合、アクセスチケットの種類および状態に対して規定されているアクセス権限に基づいてアクセス要求を許可するか否かを判定し、また状態遷移要求を受け付けた場合、アクセスチケットの種類および状態に基づいて遷移先状態を決定し、この決定した遷移先状態でアクセスチケットの状態を更新する情報アクセス制御プログラムを記録媒体に記録しているため、該記録媒体を用いて、その流通性を高めることができる。

10 【0046】請求項19記載の本発明は、請求項17記載の発明において、前記アクセスチケットの状態を更新する処理が、アクセスチケットの各状態が遷移する遷移先状態を各状態に対応して状態遷移情報格納テーブルに格納しておき、アクセス者からの前記状態遷移要求とともに入力されたアクセスチケットの状態に対応する遷移先状態を前記状態遷移情報格納テーブルから読み出し、この読み出した遷移先状態でアクセスチケットの状態を更新する情報アクセス制御プログラムを記録媒体に記録することを要旨とする。

20 【0047】請求項19記載の本発明にあっては、アクセスチケットの各状態の遷移先状態を状態遷移情報格納テーブルに格納しておき、アクセス者からの状態遷移要求の入力時、状態遷移情報格納テーブルからアクセスチケットの状態に対応する遷移先状態を読み出し、この遷移先状態でアクセスチケットの状態を更新する情報アクセス制御プログラムを記録媒体に記録しているため、該記録媒体を用いて、その流通性を高めることができる。

30 【0048】また、請求項20記載の本発明は、請求項18記載の発明において、前記アクセスチケットの状態を更新する処理が、各種類のアクセスチケットの各状態が遷移する遷移先状態をアクセスチケットの複数の種類の複数の状態の各々に対応して状態遷移情報格納テーブルに格納しておき、アクセス者から前記状態遷移要求とともに入力されたアクセスチケットの種類および状態に対応する遷移先状態を前記状態遷移情報格納テーブルから読み出し、この読み出した遷移先状態でアクセスチケットの状態を更新する情報アクセス制御プログラムを記録媒体に記録することを要旨とする。

40 【0049】請求項20記載の本発明にあっては、各種類のアクセスチケットの各状態の遷移先状態を状態遷移情報格納テーブルに格納しておき、アクセス者から状態遷移要求の入力時、アクセスチケットの種類および状態に対応する遷移先状態を状態遷移情報格納テーブルから読み出し、この遷移先状態でアクセスチケットの状態を更新する情報アクセス制御プログラムを記録媒体に記録しているため、該記録媒体を用いて、その流通性を高めることができる。

50 【0050】更に、請求項21記載の本発明は、請求項17乃至20のいずれかに記載の発明において、前記アクセスチケットの状態を更新する処理が、アクセス者か

らの前記状態遷移要求に状態遷移イベントが含まれており、この状態遷移イベントも考慮して前記遷移先状態を決定している情報アクセス制御プログラムを記録媒体に記録することを要旨とする。

【0051】請求項21記載の本発明にあつては、アクセス者からの状態遷移要求に状態遷移イベントが含まれており、この状態遷移イベントも考慮して遷移先状態を決定している情報アクセス制御プログラムを記録媒体に記録しているため、該記録媒体を用いて、その流通性を高めることができる。

【0052】請求項22記載の本発明は、請求項17または18記載の発明において、前記要求とともに入力されるアクセスチケットが有効か否かを検証する情報アクセス制御プログラムを記録媒体に記録することを要旨とする。

【0053】請求項22記載の本発明にあつては、状態遷移要求やアクセス要求等の要求とともに入力されるアクセスチケットが有効か否かを検証している情報アクセス制御プログラムを記録媒体に記録しているため、該記録媒体を用いて、その流通性を高めることができる。

【0054】また、請求項23記載の本発明は、請求項17記載の発明において、前記アクセス要求を許可するか否かを判定する処理が、アクセスチケットの各状態に対応して規定されるアクセス権限をアクセスチケット権限情報格納テーブルに格納しておき、前記アクセス要求とともに入力されるアクセスチケットの状態に対応して規定されているアクセス権限を前記アクセスチケット権限情報格納テーブルから読み出し、この読み出したアクセス権限に基づいて前記アクセス要求を許可するか否かを判定する情報アクセス制御プログラムを記録媒体に記録することを要旨とする。

【0055】請求項23記載の本発明にあつては、アクセスチケットの各状態に対応するアクセス権限をアクセスチケット権限情報格納テーブルに格納しておき、アクセス要求時、アクセスチケットの状態に対応するアクセス権限をアクセスチケット権限情報格納テーブルから読み出し、このアクセス権限に基づいてアクセス要求を許可するか否かを判定している情報アクセス制御プログラムを記録媒体に記録しているため、該記録媒体を用いて、その流通性を高めることができる。

【0056】更に、請求項24記載の本発明は、請求項18記載の発明において、前記アクセス要求を許可するか否かを判定する処理が、アクセスチケットの複数の種類の複数の状態の各々に対応して規定されるアクセス権限をアクセスチケット権限情報格納テーブルに格納しておき、前記アクセス要求とともに入力されるアクセスチケットの種類および状態に対応して規定されているアクセス権限を前記アクセスチケット権限情報格納テーブルから読み出し、この読み出したアクセス権限に基づいて前記アクセス要求を許可するか否かを判定する情報ア

セス制御プログラムを記録媒体に記録することを要旨とする。

【0057】請求項24記載の本発明にあつては、アクセスチケットの複数の種類の複数の状態の各々に対応するアクセス権限をアクセスチケット権限情報格納テーブルに格納しておき、アクセス要求時、アクセスチケットの種類および状態に対応するアクセス権限をアクセスチケット権限情報格納テーブルから読み出し、このアクセス権限に基づいてアクセス要求を許可するか否かを判定している情報アクセス制御プログラムを記録媒体に記録しているため、該記録媒体を用いて、その流通性を高めることができる。

【0058】

【発明の実施の形態】以下、図面を用いて本発明の実施の形態について説明する。図1は、本発明の一実施形態に係る情報アクセス制御方法を実施する情報アクセス制御装置の構造を示すブロック図である。

【0059】なお、本実施形態では、それぞれネットワークに接続されたユーザAの端末とユーザBの端末の間において、ユーザBの端末に格納されているユーザB所有の情報（ターゲット情報）への、ユーザAによるアクセスをユーザBの端末に設けた本発明によるアクセス制御システムによってアクセス制御する場合について述べる。

【0060】また、本実施形態では、ユーザAと、ユーザBがネットワーク上の情報伝達手段であるWorld Wide Web (WWW) や電子メール等を用いて、ネットワーク上で商品の売買を行うという場面を想定し、販売者ユーザAが、売買取引の進行に応じて、購入者ユーザBの端末に格納されているユーザBの住所や氏名などといった情報にアクセスする際のアクセス制御について述べる。

【0061】図1に示す情報アクセス制御装置について説明する。図1において、1はアクセスチケットを発行するアクセスチケット発行手段であり、2はアクセス要求を許可するかどうか判定するアクセス権限判定手段であり、3はアクセスチケットが有効なものかどうか検証するアクセスチケット検証手段であり、4はアクセスチケットの状態遷移を実施する状態遷移実施手段である。5はアクセスチケットの状態とその遷移の仕方を記述した状態遷移情報105を格納する状態遷移情報格納手段であり、6はアクセスチケットの各状態に対応するアクセス権限を記述したアクセスチケット権限情報106を格納するアクセスチケット権限情報格納手段であり、7は有効なアクセスチケットに関する情報である有効アクセスチケット情報107を格納する有効アクセスチケット情報格納手段であり、8はターゲット情報108を格納するターゲット情報格納手段である。

【0062】また、9はアクセス制御システムを備えたユーザBの対話型端末であり、10はDES (Data Encryption Standard) などの対称型暗号方式による共通鍵

であってアクセスチケットの生成および検証に用いられるアクセスチケット生成検証鍵 k_{110} を格納するアクセスチケット生成検証鍵格納手段であり、11はアクセスチケットの生成および検証に補助的に用いられるアクセスチケット生成検証補助データ d_{111} を格納するアクセスチケット生成検証補助データ格納手段であり、12はターゲット情報108に対してアクセスを行うアクセス者ユーザAの端末であり、13はターゲット情報所有者の端末9およびアクセス者の端末12などを結ぶ通信ネットワークであり、14は本発明によるアクセス制御の処理手順が記述されたプログラムであり、15はプログラム14に基づき処理を行う機能を有するCPUである。

【0063】また、図2は、図1の有効アクセスチケット情報格納手段7に格納された有効アクセスチケット情報107のある時点での登録内容を示しており、有効なアクセスチケットそれぞれについて、アクセスチケットを一意に識別するアクセスチケットIDと、アクセスチケット種別と、その時点における状態を保持している。

【0064】図3は、図1の状態遷移情報格納手段5に格納された状態遷移情報105の内容を示しており、アクセスチケットの種別毎に、取り得る状態311、初期状態312、状態遷移規則313、最終状態314が記述される。また、各状態遷移規則は遷移元状態321、状態遷移イベント名称322、遷移先状態323から構成される。

【0065】図4は、図1のアクセスチケット権限情報格納手段6に格納されたアクセスチケット権限情報106の内容を示しており、アクセスチケットの種別毎に、取り得る状態それぞれに対応するアクセス権限が記述される。また、各アクセス権限は、ターゲット情報の識別子とそれに対するアクセス種別の組で構成される。

【0066】図5は、図1のターゲット情報格納手段8に格納されたターゲット情報108の内容を示しており、階層化された項目501と、それぞれの項目に対応する情報(値)502とで構成される。

【0067】次に、上述したように構成される本実施形態の情報アクセス制御装置の作用を説明する。なお、この説明では、アクセスチケット情報の所有者であるユーザBは予めアクセスチケットの種別毎にその状態遷移情報105およびアクセスチケット権限情報106を記述し、それぞれ状態遷移情報格納手段5およびアクセスチケット権限情報格納手段6に格納しているものとする。また、状態遷移情報105およびアクセスチケット権限情報106はそれぞれ図3、図4に示すように定義されているものとする。

【0068】まず、アクセスチケットの発行について図6に示すフローチャートを参照して説明する。

【0069】本実施形態では、ターゲット情報所有者のユーザBは、アクセス者のユーザAによるアクセスに先

だって、ユーザAに許容すべき適切なアクセス権限と対応するアクセスチケットを与えるため、適切なアクセスチケットの種別を指定して、アクセス制御システムにアクセスチケットの生成を命じる。

【0070】これは例えば、ユーザBがユーザAの開設するWWW上の仮想的な商店であるホームページ(電子ショップ)を訪れた時点などで行われる。

【0071】本発明によれば、アクセスチケットの生成を指示されたアクセス制御システムはアクセスチケット発行手段1を用いて、指定された種別を持つアクセスチケットを新規に生成し、出力する。

【0072】図6に示すアクセスチケット発行手続きでは、まず、ステップS602で、指定されたアクセスチケットの種別 $type1$ を取得し、ステップS603で新しくユニークなアクセスチケットID $id1$ を払い出す。

【0073】ここで、アクセスチケットIDの生成・払出の方法としては、アクセスチケットIDの検索を容易にするため、またアクセスチケットIDを格納する領域が小さくて済むように、アクセスチケットIDのデータサイズが可能な限り小さいものであるようにする必要がある。このため、本実施形態では、ステップS603におけるアクセスチケットIDの生成・払出の方法として、0(ゼロ)から連続した整数値を払い出す方法を採用している。

【0074】そして、ステップS604、ステップS605で、アクセスチケット生成検証補助データ d_{111} と、アクセスチケット生成検証鍵 k_{110} とを取得し、ステップS606で(アクセスチケットID $id1$ 、アクセスチケット生成検索補助データ d_{111})なる形式のデータを鍵 k_{110} で暗号化し、これを新規アクセスチケット $t1$ とする。

【0075】その後、ステップS607で、状態遷移情報105から、アクセスチケット種別 $type1$ に対応する状態遷移情報 $s11$ を取得し、ステップS608で、 $s11$ から初期状態 $s1$ を取得する。

【0076】そして、ステップS609で、アクセスチケット種別 $type1$ と、初期状態 $s1$ とともに、アクセスチケットID $id1$ を、有効アクセスチケット情報107に記録した後、ステップS610で、同アクセスチケット $t1$ を出力する。出力されたアクセスチケットの構造を図13に示す。

【0077】ここで、状態遷移情報105が図3に示す状態であり、また、生成するアクセスチケットの種別として、“購入取引1”が指定され、また、ステップS603においては新規アクセスチケットIDとして、0001が払い出されるとすると、上記手順により、図3に示す状態遷移情報105の内容に基づいて、“購入取引1”を一種別とし、“閲覧中”をその状態とするアクセスチケット $t12$ が生成され、その情報が有効アクセス

10

20

30

40

50

チケット情報107に登録される。

【0078】ここで、t2は、払い出されたアクセスチケットID0004と、アクセスチケット生成検証補助データd111を（アクセスチケットID0004、アクセスチケット生成検証補助データd111）の形式にしたものをアクセスチケット生成検証鍵k110で暗号化したものである。

【0079】同アクセスチケットt2が有効アクセスチケット情報107に登録された様子を図12に示す。

【0080】このようにして、アクセスチケットt2が10発行されると、ユーザBは、SSL（Secure Socket Layer）などによりユーザAとの間で安全な通信路を確立した上で、同アクセスチケットを送信する。

【0081】次に、アクセス要求処理、アクセスチケット検証処理、アクセス権限判定処理について図8、図9、図10のフローチャートを参照して説明する。

【0082】本実施形態では、アクセス者であるユーザAは、ユーザBの情報（ターゲット情報）にアクセスする際に、そのアクセスの内容を示すアクセス要求と、先にユーザBから取得していたアクセスチケットとを安全な通信路を介してアクセス制御システムに送信する。20

【0083】アクセス制御システムにおけるアクセス要求処理手続きを図8を用いて詳細に説明する。

【0084】まず、ステップS802、ステップS803で、受信したアクセス要求req1とアクセスチケットt1とをそれぞれ取得する。そして、ステップS804で、アクセスチケットt1が有効かどうかをアクセスチケット検証手段3を用いて判定する。

【0085】このアクセスチケット検証手続きを図7を用いてより詳細に説明する。

【0086】まず、ステップS702で、アクセスチケットt1を取得し、ステップS703でアクセスチケット生成検証鍵k110を取得する。次いで、ステップS704で、t1に対してk110による復号化を試み、失敗した場合には、同アクセスチケットt1を無効と判定する（ステップS709）。

【0087】復号できた場合は、その結果得られたデータをm1とし（ステップS705）、ステップS706でアクセスチケット生成検証補助データd111を取得し、ステップS707で、m1＝（アクセスチケットIDid1、アクセスチケット生成検証補助データd111）なるアクセスチケットIDが有効アクセスチケット情報107に登録されているか確認する。登録されていない場合は、アクセスチケットt1を無効と判定する（ステップS709）。登録されていれば、同アクセスチケットIDid1をアクセスチケットt1のアクセスチケットIDとして一時的に（アクセス要求処理手続きが終わるまでの間）保存し、アクセスチケットt1を有効と判定する（ステップS708）。

【0088】上記アクセスチケット検証手続きによって 50

アクセスチケットt1が無効と判定された場合、アクセス制御システムは、アクセス要求req1を拒否し、これに対する処理を終了する。有効と判定された場合には、アクセス要求req1を拒否するか否かをアクセス権限判定手段2を用いて判定する（ステップS805）。

【0089】この手続きを図9を用いてより詳細に説明する。

【0090】まず、ステップS902、ステップS903で、アクセス要求req1とアクセスチケットt1をそれぞれ取得し、ステップS904で、有効アクセスチケット情報107から、アクセスチケットt1に対応するアクセスチケット種別type1と、その時点におけるアクセスチケットt1の状態s1を取得し、ステップS905で、アクセスチケット権限情報106から種別type1に対応するアクセスチケット権限情報ri1を取得し、ステップS906で、アクセスチケット権限情報ri1から、アクセスチケットt1の状態s1に対応するアクセス権限R1を取得し、これを、その時点で、アクセスチケットt1に対応するアクセス権限と決定する。

【0091】そして、ステップS907で、アクセス権限R1が、アクセス要求req1で示されるアクセス内容に含まれているかどうかを検査する。含まれない場合、アクセス権限R1は、アクセス要求req1に対して無効であり、同アクセス要求req1を不許可とする（ステップS909）。含まれていれば、許可と判定する（ステップS908）。

【0092】アクセス権限判定手段2によってアクセス要求req1が不許可と判定された場合、アクセス制御システムは、同アクセス要求req1を拒否し、これに対する処理を終了する。有効と判定された場合には、ステップS806で、アクセス要求req1の内容を処理し、その返答をユーザAに安全な通信路を介して送信する。

【0093】ここで、本実施形態においては、ユーザAが、ユーザBの端末9のアクセス制御システムに対して、「年齢の参照」というアクセス要求req2を、予め取得してあったアクセスチケットt2とともに送信したとする。

【0094】また、この時の有効アクセスチケット情報107の登録内容は、図12に示す通りであり、アクセスチケット権限情報106の内容は、図4に示す通りであるとす。

【0095】まず、アクセス制御システムは、アクセス要求req2（＝「年齢：参照」）とアクセスチケットt2とを取得し（ステップS802、ステップS803）、アクセスチケットt2が有効かどうかを、アクセスチケット検証手段3を用いて判定する（ステップS804）。

【0096】アクセスチケット検証手段3では、上述の
手順（ステップS701～ステップS708）により、
アクセスチケットt2は、アクセスチケットID000
4を持つ有効なアクセスチケットと判定される。

【0097】アクセスチケットt2が有効と判定され
たので、次に、アクセス権限判定手段2を用いて、アクセ
ス要求req2を許可するかどうかを判定する（ステッ
プS805）。

【0098】アクセス権限判定手段2では、上述の手順
の通り、アクセス要求req2とアクセスチケットt2
とを取得し（ステップS902、ステップS903）、
図12に示す有効アクセスチケット情報107の登録内
容から、t2の種別“購入取引1”と、状態“閲覧中”
を取得する（ステップS904）。

【0099】次に、図4に示すアクセスチケット権限情
報106から、アクセスチケットt2の種別“購入取引
1”に対応するアクセスチケット権限情報を取得し（ス
テップS905）、これから、状態“閲覧中”に対応す
るアクセス権限（図4の）401を取得し、これをアクセ
スチケットt2に対応するアクセス権限として決定す
る（ステップS906）。

【0100】そして、同アクセス権限401が、アクセ
ス要求req2の内容「年齢：参照」を含むことから、
アクセス要求req2に対して有効であることになり、
アクセス要求req2に許可の判定を下す（ステップS
907、ステップS908）。

【0101】アクセス要求req2が許可と判定され
たので、最後にこの内容を処理する。すなわち、ユーザB
の年齢が、ターゲット情報108から読み出され、ユー
ザAに安全な通信路を介して返信される（ステップS
806）。

【0102】次に、状態遷移について図10、図11の
フローチャートを参照して説明する。

【0103】本実施形態では、アクセス者のユーザA、
もしくは、ターゲット情報所有者のユーザBは、両者の
取引の局面が変化するとともに、ユーザAに付与されて
いるアクセスチケットの状態を更新し、対応するアクセ
ス権限を変更するために、アクセスチケットと状態遷移
イベント名称を指定した状態遷移要求をアクセス制御シ
ステムに安全な通信路を介して送信する。

【0104】アクセス制御システムにおける状態遷移要
求処理手続きを図10を用いて詳細に説明する。

【0105】アクセス制御システムは、まずステップS
1002、ステップS1003で、受信した状態遷移要
求sreq1から、状態遷移イベント名称e1とアクセ
スチケットt1とをそれぞれ取得する。そして、ステッ
プS1004で、アクセスチケットt1が有効かどうか
を、アクセスチケット検証手段3を用いて判定する。こ
の手続きは、既に説明した通りであるので省略する。

【0106】アクセスチケット検証手続きによってアク

セスチケットt1が無効と判定された場合、アクセス制
御システムは、状態遷移要求sreq1を拒否し、これ
に対する処理を終了する。有効と判定された場合には、
上記イベント名称e1とアクセスチケットt1とを状態
遷移実施手段4に入力し、状態遷移実施手続きを実行さ
せる（ステップS1005）。

【0107】この手続きを図11を用いてより詳細に説
明する。

【0108】状態遷移実施手段4では、ステップS11
02、ステップS1103で、状態遷移イベント名称e
1とアクセスチケットt1とをそれぞれ取得し、ステッ
プS1104で、有効アクセスチケット情報107より、
アクセスチケットt1に対応する種別type1
と、その時点におけるアクセスチケットt1の状態s1
を取得し、ステップS115で、状態遷移情報105か
ら、アクセスチケット種別type1に対応する状態遷
移情報s11を取得する。

【0109】次に、ステップS1106で、状態s1を
遷移元状態とし、イベント名称e1を遷移イベントとす
る状態遷移規則が、状態遷移情報s11に存在するか調
べる。もし存在しなければ、状態遷移要求sreq1に
対する状態遷移実施手続きを終了する。この場合、アク
セスチケットt1の状態の変更は一切行われない。

【0110】もし上記状態遷移規則が存在すれば、これ
を状態遷移規則rule1として取得する（ステップS
1107）。

【0111】そして、ステップS1108で、有効アク
セスチケット情報107に保持されているアクセスチケ
ットt1の状態を、状態遷移規則rule1で指定され
ている遷移先状態s2に更新する。

【0112】更に、ステップS1109で、アクセスチ
ケットt1の遷移後の状態s2が、状態遷移情報s11
において最終状態として定義されているかどうかを検査
する。もし最終状態として定義されていれば、有効アク
セスチケット情報107からアクセスチケットt1に関
するすべての項目を削除して上記アクセスチケットを無
効化し（ステップS1110）、状態遷移実施手続きを
終了する。e1が最終状態として定義されていなければ、
そのまま状態遷移実施手続きを終了する。

【0113】ここで、本実施形態においては、ユーザB
が、ユーザAに対して商品購入の申込を行い、これに合
わせて、ユーザAが、“購入”というイベント名称と、
予め取得してあったアクセスチケットt2からなる状態
遷移要求sreq2を、ユーザBの端末9のアクセス制
御システムに送信したとする。

【0114】また、この時の有効アクセスチケット情報
107の内容は図12に示す通りであり、状態遷移情報
105の内容は、図3に示す通りであるとする。

【0115】まず、アクセス制御システムは、イベント
名称“購入”とアクセスチケットt2とを取得し（ステ

ップS1002、ステップS1003)、アクセスチケットt2が有効かどうかを、アクセスチケット検証手段3を用いて判定する(ステップS1004)。

【0116】アクセスチケット検証手段3では、既に述べた手順(ステップS701～ステップS708)により、アクセスチケットt2は、アクセスチケットID0004を持つ有効なアクセスチケットと判定される。

【0117】次に、上記イベント名称“購入”とアクセスチケットt2とを状態遷移実施手段4に入力し、状態遷移実施手続きを実行させる(ステップS1005)。

【0118】状態遷移実施手段4では、上述の手順の通り、イベント名称“購入”とアクセスチケットt2とを取得し(ステップS1102、ステップS1103)、図12に示す有効アクセスチケット情報107の登録内容から、t2の種別“購入取引1”と、状態“閲覧中”を取得する(ステップS1104)。

【0119】次に、図3に示す状態遷移情報105から、アクセスチケットt2の種別“購入取引1”に対応する状態遷移情報を読み出し(ステップS1105)、これから、状態“閲覧中”を遷移元状態とし、イベント“購入”を遷移イベントとする状態遷移規則(図3の)301を取得し(ステップS1106、ステップS1107)、有効アクセスチケット情報107に保持されているアクセスチケットt2の状態を、同状態遷移規則301で指定されている遷移先状態“注文中”に更新する(ステップS1108)。

【0120】更に、アクセスチケットt2の遷移後の状態“注文中”が、最終状態として定義されているかどうか検査する(ステップS1109)。同状態は、最終状態として定義されていないので、そのまま状態遷移実施

【0121】この時点におけるアクセスチケットt2の状態“注文中”に対応するアクセス権限は、図4に示すアクセスチケット権限情報106から、アクセス権限402となり、先ほどアクセス要求処理手続きについて述べた際に、アクセスチケットt2に対応していたアクセス権限(図4の)401とは異なっていることがわかる。

【0122】このように、状態遷移要求によってアクセスチケットの状態を変更させることより、同じアクセスチケットに対するアクセス権限を容易に変更することができる。すなわち、同一のアクセス者に対して許容するアクセス権限をアクセスチケットを再発行・再付与することなく、容易に変更することができる。

【0123】上述したように、本実施形態では、複数の状態の各々について異なるアクセス権限を対応づけたアクセス権限決定補助データ(アクセスチケット)を発行してアクセス者に付与し、取引上の局面の変化に応じて送付される状態遷移イベントを元に同アクセスチケットの状態を変更することにより、取引上の局面の変化に

じて、同アクセスチケットに対応するアクセス権限、すなわち、同アクセスチケットを保持するアクセス者に対して許容するアクセス権限を変更する。

【0124】このため、ケイパビリティを用いた場合には、例えば同一取引の同一アクセス者に対しても局面毎に複数のケイパビリティを発行し付与する必要があったが、本発明によれば、アクセスチケットの発行・付与は一度で済む。よって、これらの発行・付与のコストが大幅に軽減される。

【0125】また同様に、ケイパビリティを用いた場合には、局面毎に与えた複数のケイパビリティの有効/無効を制御・管理する必要があったが、本発明によれば、1つのアクセスチケットの状態を制御・管理するので、それらの制御・管理の煩雑さが軽減される。

【0126】また同様に、ケイパビリティを用いた場合には、アクセス者は、局面毎に与えられた複数のケイパビリティを保持し、また局面に応じて使い分けなければならなかったが、本発明によれば、アクセス者は1つのアクセスチケットを保持し、これを用いればよいので、それら管理・利用のコストが大幅に軽減される。

【0127】上記実施形態において、アクセスチケットの生成方法として、アクセスチケットIDに固定のデータ(アクセスチケット生成検証補助データd111)を組み合わせたデータに対し、秘密の鍵により暗号化を施したものをアクセスチケットとして用いる方法(方法A)を取っているが、これは、以下の点で有利である。

【0128】まず、前途の通り、検索の効率や格納領域の節約のために、アクセスチケットIDのデータサイズは十分小さい必要があるが、そうした場合、アクセスチケットIDをそのままアクセスチケットとする方法(方法B1)、あるいは、アクセスチケットIDに固定のデータを付加してアクセスチケットとする方法(方法B2)では、あるアクセスチケットIDから別のアクセスチケットIDが類推される畏が高くなる。すなわち、あるアクセスチケットから、別のアクセスチケットが類推され、偽造される畏が高くなる。

【0129】これに対し、本方法Aでは、アクセスチケットIDに、データサイズが小さくとも、十分な長さのアクセスチケット生成検証補助データd111を付加して暗号化を施せば、あるアクセスチケットから他のアクセスチケットを類推することは困難となる。

【0130】また、上記実施形態では、アクセスチケット生成検証鍵k110として、対称型暗号方式による共通鍵を用いたが、同アクセスチケット生成検証鍵k110の代わりに、RSAなどの非対称型暗号方式による鍵の鍵対(ペア)を用意し、アクセスチケット生成手続きの際には公開鍵対の暗号化鍵を、アクセスチケット検証手続きの際には、もう一方の復号化鍵を用いることとして、アクセス制御システムを構成することもできる。

【0131】更に、上記実施形態では、アクセスチケッ

10

20

30

40

50

ト生成検証鍵k110とアクセスチケット生成検証補助データd111を固定的なデータとしたが、1つのアクセスチケット、あるいはいくつかのアクセスチケットを発行する毎に、これらを新しいものにそれぞれ変更し、アクセスチケット検証時には、同アクセスチケットの発行の際に用いたアクセスチケット生成検証鍵k110とアクセスチケット生成検証補助データd111を取得して用いる方法・構成を取ることも可能である。

【0132】この方法によれば、各アクセスチケット、もしくは、いくつかのアクセスチケットの組と、その生成に用いたアクセスチケット生成検証鍵k110とアクセスチケット生成検証補助データd111の組とを対応づける情報を生成・保持する必要があるものの、アクセスチケットの偽造をより困難なものとするため、場合によっては便利である。

【0133】また、上記実施形態では、ユーザAから状態遷移要求が送られたが、状態遷移要求は、ユーザA（すなわちアクセス者）、あるいはユーザB（すなわちターゲット情報の所有者）のいずれによって送られてもよい。

【0134】逆に、状態遷移要求が、ユーザA、ユーザBどちらから送られたものなのかを判定し、それに応じて、状態遷移するか否かを判定することは、アクセス者や、ターゲット情報のアクセス者による不適切な状態遷移要求の送付によるアクセス権限の不正な変更を防止することができるため、便利である。

【0135】これは、状態遷移情報105内の各状態遷移規則に、イベント元条件という項目を設け、“ターゲット情報所有者”、あるいは、“アクセス者”と記述するようにしておき、状態遷移実施手段4において実行される状態遷移実施手続きのステップS1108において対象のアクセスチケットt1の状態を変更する前に、入力された状態遷移要求sreq1が、ターゲット情報所有者とアクセス者、いずれから送信されたのかその送信元を識別し、同送信元と状態遷移規則rule1のイベント元条件を比較し、一致しなかった場合には、状態遷移要求sreq1を拒否し、これに対する処理を中止するように設計・構成することによって実現できる。

【0136】また、ユーザAとユーザBとの上記取引の状況を監視し、局面の変化が起こった際にそれを自動的に検知し、ユーザAに付与したアクセスチケットに対する適切な状態遷移要求をアクセス制御システムに送信するソフトウェアプロセスを用いると、より便利である。これは例えば、ユーザDがユーザAの電子ショップにアクセスするために用いるWWW閲覧用ソフトウェア（ブラウザ）に組み込まれ、ユーザBの操作を監視し、その操作に応じて取引の局面の変化を検知し、状態遷移要求を送るようなブラウザの補助ソフトウェアなどを用いることができる。

【0137】なお、上述した実施形態の説明において、

アクセスチケット等の情報を安全な通信路を介して送信するという記載における安全な通信路とは、第三者による盗聴、改竄などに対する防御措置が取られた通信路であり、既存の任意の暗号技術によって実現される。この通信路としては、例えば、インターネット上の情報流通システムであるWorld Wide Webで普及しているSSL（Secure Socket Layer）などが用いられる。

【0138】

【発明の効果】以上説明したように、本発明によれば、各状態毎にターゲット情報へのアクセス権限を規定しているアクセスチケットを各アクセス者に発行し、アクセス要求の受付時に、アクセスチケットの状態に対するアクセス権限に基づいてアクセス要求を許可するか否かを判定し、状態遷移要求の受付時、アクセスチケットの状態に基づいて遷移先状態を決定し、この遷移先状態でアクセスチケットの状態を更新するので、アクセス者に対して許容するアクセス権限を取引の局面の変化に応じて容易に変更でき、柔軟なアクセス制御を実現することができる。

【0139】また、本発明によれば、複数の種類の複数の状態の各々毎にターゲット情報へのアクセス権限を規定しているアクセスチケットを各アクセス者に発行し、アクセス要求の受付時、アクセスチケットの種類および状態に対するアクセス権限に基づいてアクセス要求を許可するか否かを判定し、また状態遷移要求の受付時、アクセスチケットの種類および状態に基づいて遷移先状態を決定し、この遷移先状態でアクセスチケットの状態を更新するので、アクセス者に対して許容するアクセス権限を取引の局面の変化に応じて容易に変更でき、柔軟なアクセス制御を実現することができる。

【図面の簡単な説明】

【図1】本発明の一実施形態に係る情報アクセス制御方法を実施する情報アクセス制御装置の構成を示すブロック図である。

【図2】図1に示す情報アクセス制御装置で使用される有効アクセスチケット情報の登録内容例を示す説明図である。

【図3】図1に示す情報アクセス制御装置で使用されている状態遷移情報格納手段に格納された状態遷移情報の内容を示す説明図である。

【図4】図1に示す情報アクセス制御装置で使用されているアクセスチケット権限情報格納手段に格納されているアクセスチケット権限情報の内容を示す説明図である。

【図5】図1に示す情報アクセス制御装置で使用されているターゲット情報格納手段に格納されているターゲット情報の内容を示す説明図である。

【図6】図1に示す情報アクセス制御装置のアクセスチケット発行手段におけるアクセスチケット発行手続きを示すフローチャートである。

【図7】図1に示す情報アクセス制御装置のアクセスチケット検証手段におけるアクセスチケット検証手続きを示すフローチャートである。

【図8】図1に示す情報アクセス制御装置のアクセス要求処理手続きを示すフローチャートである。

【図9】図1に示す情報アクセス制御装置のアクセス権限判定手段におけるアクセス権限判定手続きを示すフローチャートである。

【図10】図1に示す情報アクセス制御装置の状態遷移要求処理手続きを示すフローチャートである。

【図11】図1に示す情報アクセス制御装置の状態遷移実施手段における状態遷移実施手続きを示すフローチャートである。

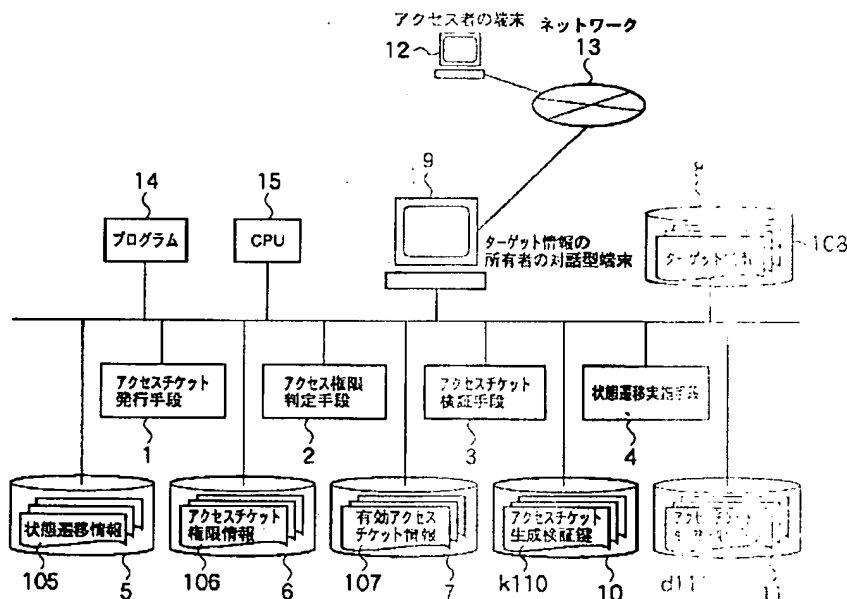
【図12】図1に示す情報アクセス制御装置で使用される有効アクセスチケット情報の登録内容を示す説明図である。

* 【図13】図1に示す情報アクセス制御装置におけるアクセスチケット発行手続きにより生成されたアクセスチケットの構造を示す説明図である。

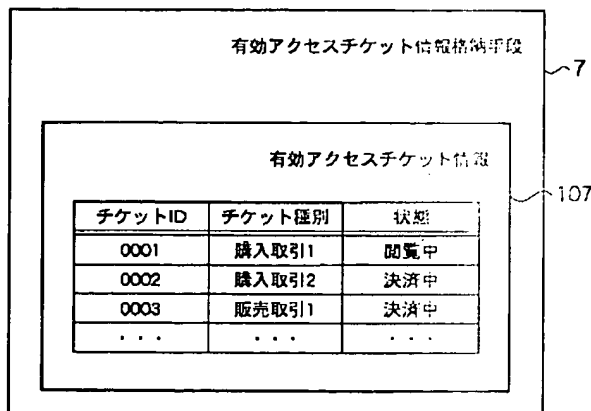
【符号の説明】

- 1 アクセスチケット発行手段
- 2 アクセス権限判定手段
- 3 アクセスチケット検証手段
- 4 状態遷移実施手段
- 5 状態遷移情報格納手段
- 6 アクセスチケット権限情報格納手段
- 7 有効アクセスチケット情報格納手段
- 8 マーケット情報格納手段
- 9 マーケット情報所有者の端末
- 10 アクセスチケット生成検証鍵格納手段
- 11 アクセスチケット生成検証補助データ格納手段

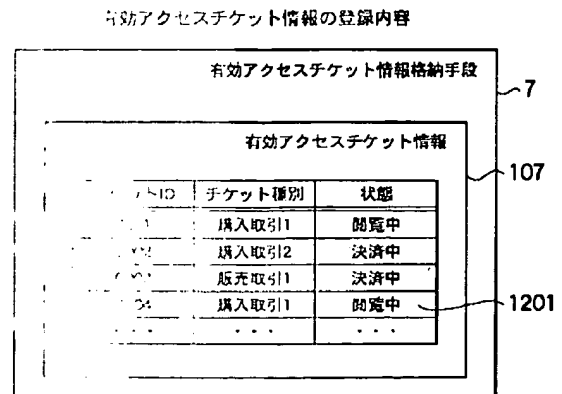
【図1】



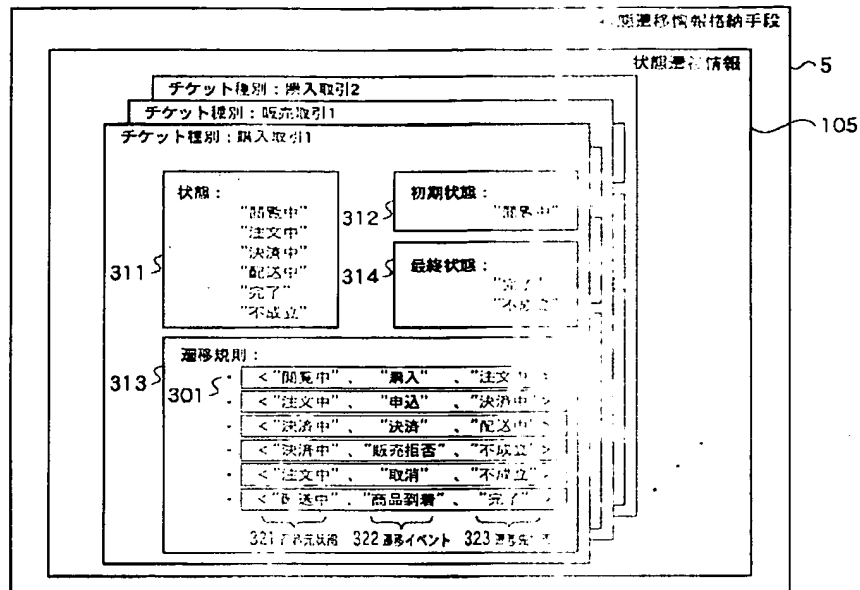
【図2】



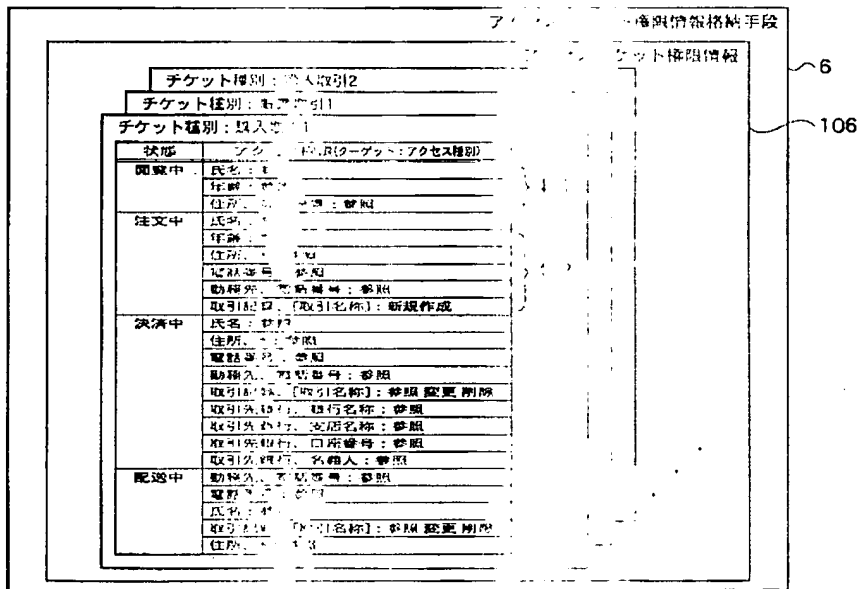
【図12】



【図3】



【図4】



【図5】

アクセスチケット発行手段により生成された
アクセスチケット

1301	d111
(アクセスチケットID、アクセスチケット生成履歴用補助データ)	
暗号化 [アクセスチケットID] [暗号]	

【図5】

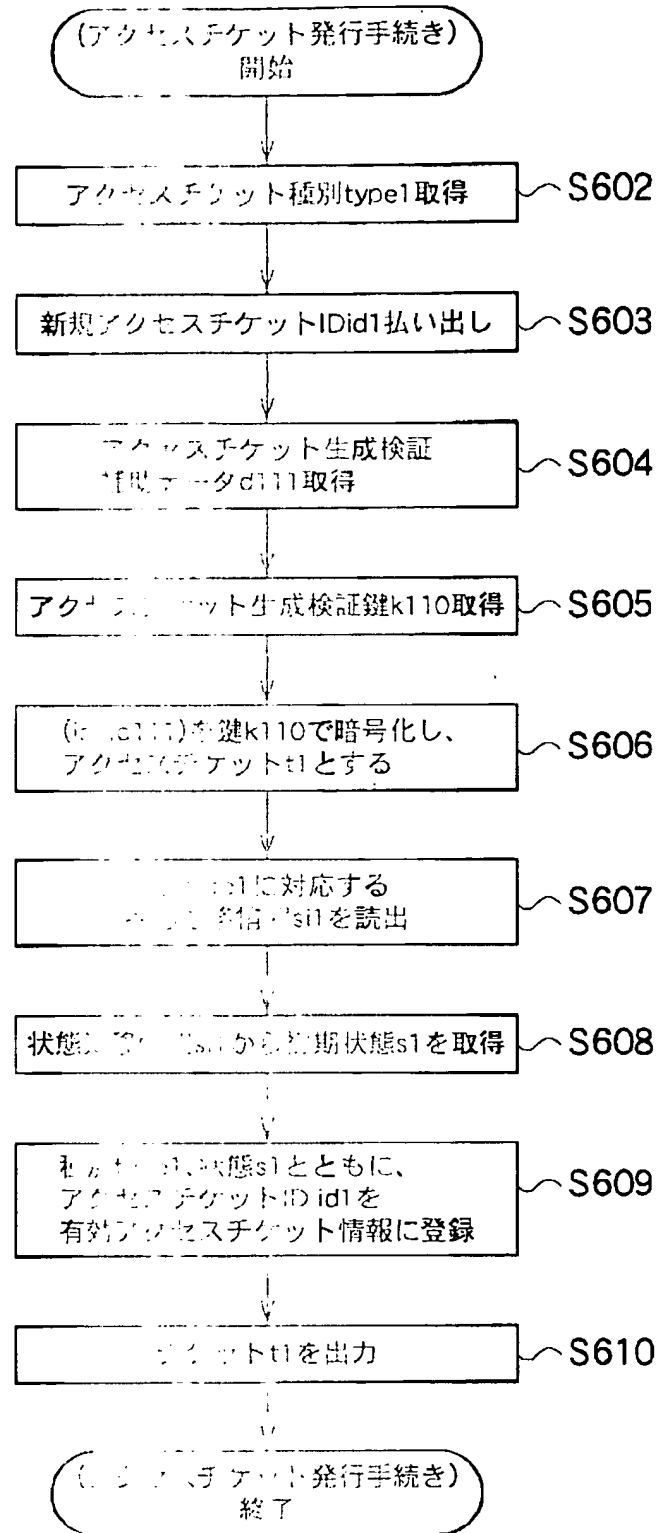
108 8

ターゲット情報 登録手段

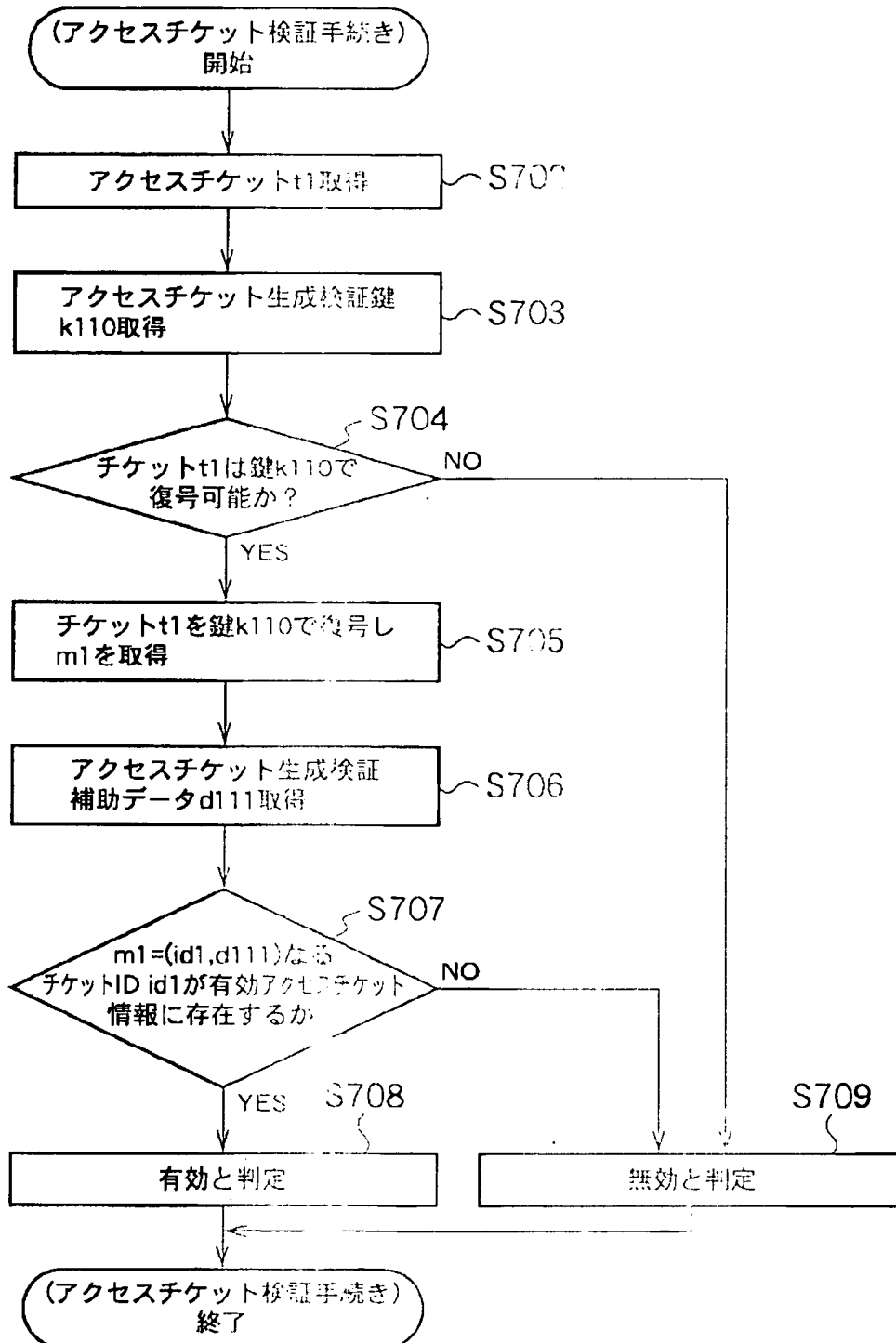
501 502

項目	値
コンタクト情報	
年齢	38
電話番号	30-1234-5678
氏名	寺田 純
電子メールアドレス	itun@100.bar
ファックス番号	03-1234-5678
住所	
郵便番号	123-4567
都道府県	東京都
市区町村	大田区
...	...
勤務先	
会社名	寺田株式会社
部署名	総務部
電話番号	03-8765-4321
ファックス番号	03-8765-4321
住所	
郵便番号	987-6543
都道府県	東京都
市区町村	大田区
...	...
取引先銀行	
名義人	寺田 純
支店名称	大田支店
口座番号	1234567
銀行名称	寺田銀行
...	...
個人情報	
誕生日	年 1962
	月 1
	日 1
結婚/未婚	既婚
...	...
取引記録	
取引1	名称 雑貨購入
	日時 1998.10.10
...	...
...	...

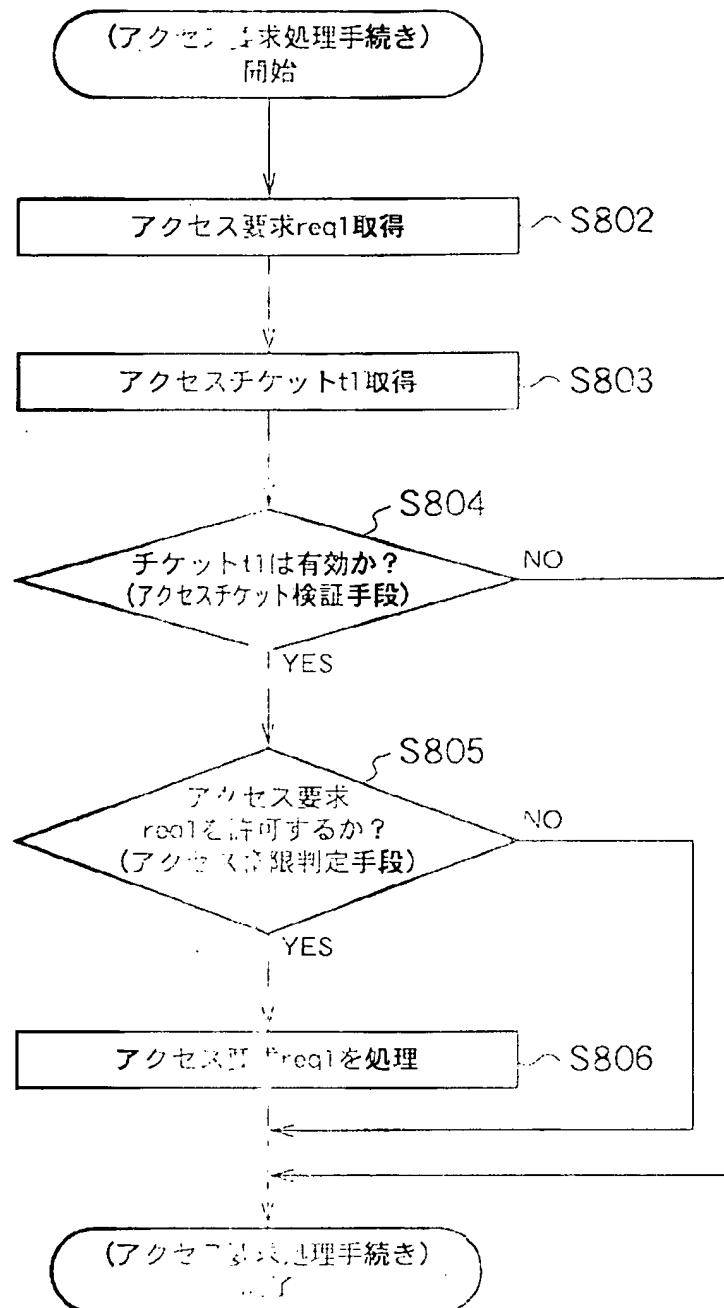
【図6】



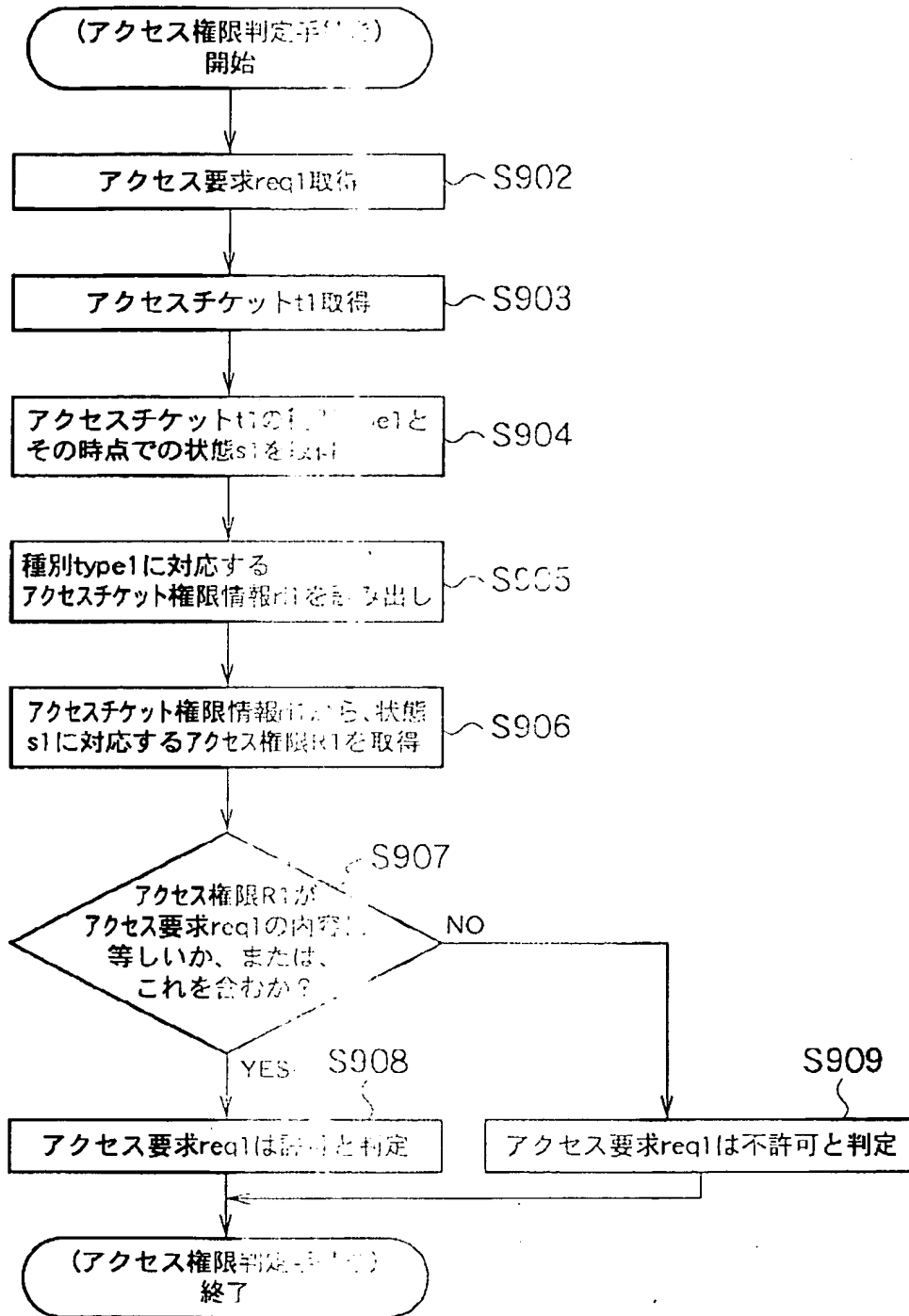
【図7】



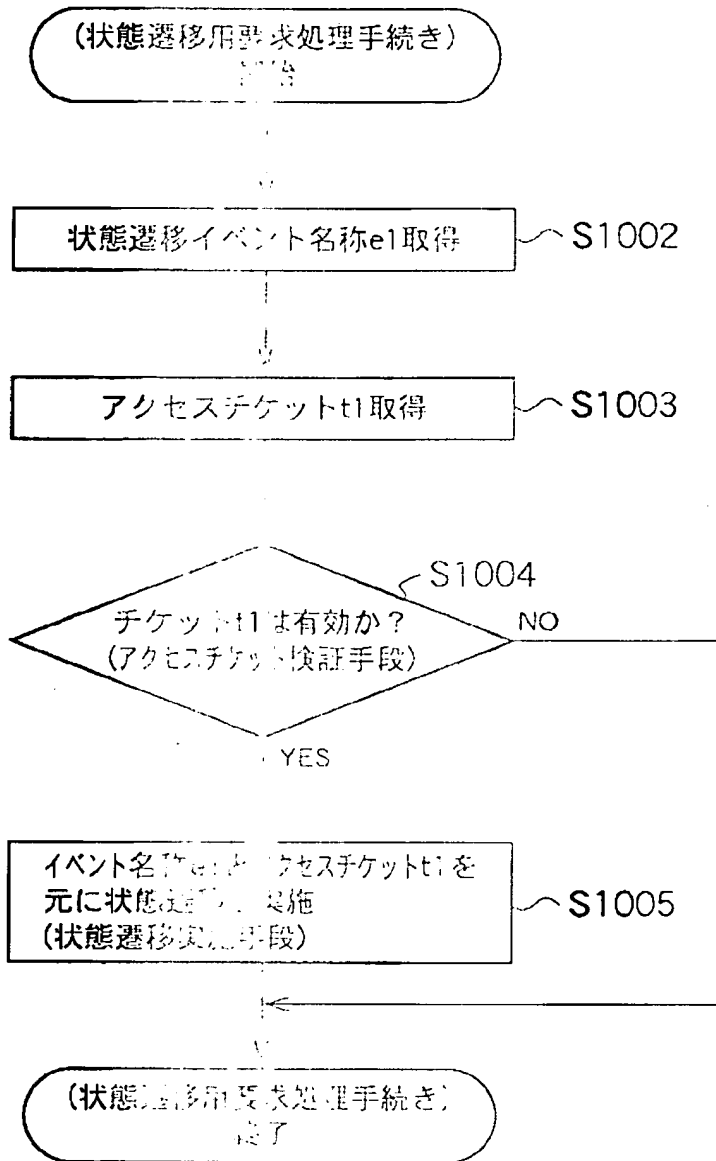
【図8】



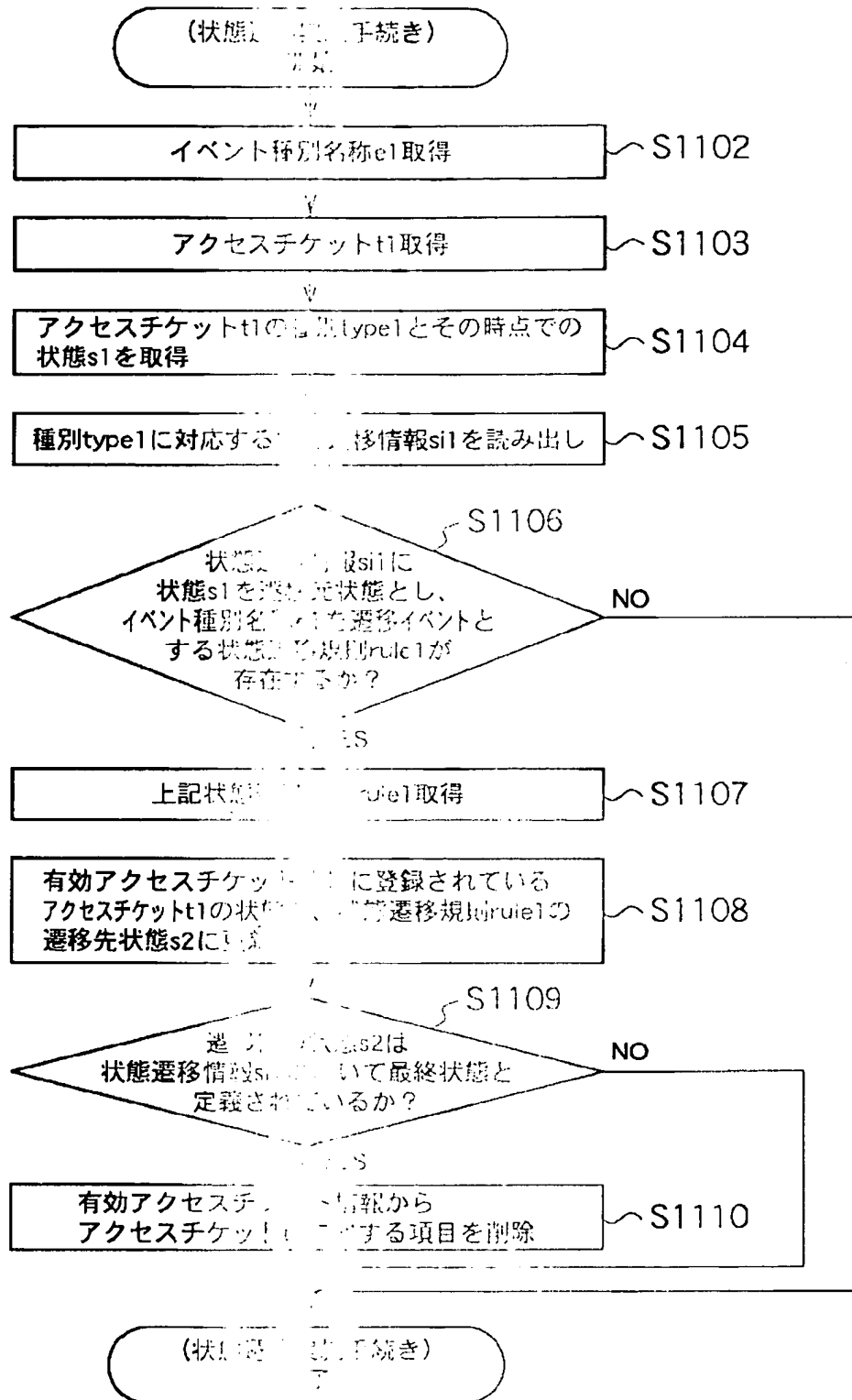
【図9】



【図10】



【図11】



フロントページの続き

Fターム(参考) 5B017 AA01 BA05 BAC7 BB01 CC03
BB07 CA16
5B049 BB11 CC02 CC05 EE01 FF02
GG04 GG07 GG15
5B085 AA08 AE08 AE18 AE28
BE07 BG06
5J104 AA07 KA01 KA04 KAC7 LA07
NA36 PA07 PA10
9A001 JJ18 JJ25 JZ07 JJ01